ProtectTools

お使いになる前に

目次

4 Embedded Security for ProtectTools

5 BIOS Configuration for ProtectTools

6 Credential Manager for ProtectTools

1　概要

ProtectTools Security Manager には、コンピュータ、ネットワーク、および重要なデータに対する不正アクセス防止に役立つセキュリティ機能があります。次のソフトウェア モジュールによって、セキュリティ機能が強化されます。

- Smart Card Security for ProtectTools
- Java Card Security for ProtectTools
- Embedded Security for ProtectTools
- BIOS Configuration for ProtectTools
- Credential Manager for ProtectTools

使用しているコンピュータで利用可能なソフトウェア モジュールは、モデルによって異なります。たとえば、Embedded Security for ProtectTools を使用するには、トラステッド プラットフォーム モジュール (TPM) 内蔵セキュリティ チップ (一部のモデルのみ) がコンピュータにインストールされている必要があります。また、Smart Card Security for ProtectTools を使用するには、オプションのスマート カードとリーダーが必要です。

ProtectTools ソフトウェア モジュールは、プリインストールされているか、プリロードされているか、HP の Web サイトからダウンロードできます。詳しくは、http://www.hp.com/jp を参照してください。

注記　このガイドでは、該当する ProtectTools ソフトウェア モジュールをインストール済みであることを前提に説明しています。

ProtectTools セキュリティ マネージャへのアクセス

Microsoft® Windows® コントロール パネルから ProtectTools セキュリティ マネージャにアクセスするには、次の手順を行います。

▲ **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。

注記 Credential Manager モジュールを構成した後、Windows ログオン画面から Credential Manager に直接ログオンして ProtectTools を開くこともできます。詳しくは、第 6 章「Credential Manager for ProtectTools」の「Credential Manager を使用した Windows へのログオン」を参照してください。

セキュリティ ロールについて

コンピュータ セキュリティを管理する際 (特に大規模な組織の場合)、さまざまな種類の管理者およびユーザーの間で責任と権限を分割することが重要です。

注記 小規模な組織や個人使用の場合は、これらの役割のすべてを同じユーザーが実行することがあります。

ProtectTools では、セキュリティの任務と権限を次の役割 (ロール) に分割できます。

- セキュリティ オフィサ - 会社またはネットワークのセキュリティ レベルを定義し、展開するセキュリティ機能 (スマート カード、バイオメトリック リーダー、USB トークンなど) を決定します。

注記 ProtectTools の機能の大半は、企業のセキュリティ オフィサが HP と協力してカスタマイズできます。詳しくは、http://www.hp.com/jp を参照してください。

- IT 管理者 - セキュリティ オフィサが定義したセキュリティ機能を適用し、管理します。一部の機能の有効化と無効化も実行できます。たとえば、セキュリティ オフィサがスマート カードを展開することを決定した場合、IT 管理者はスマート カードの BIOS セキュリティ モードを有効にすることができます。
- ユーザー - セキュリティ機能を使用します。たとえば、セキュリティ オフィサと IT 管理者がシステムでスマート カードを有効にした場合、ユーザーはスマート カードの PIN を設定し、認証のためにカードを使用できます。

ProtectTools パスワードの管理

ProtectTools セキュリティ マネージャの機能の大半は、パスワードによって保護されています。よく使用されるパスワード、パスワードを設定するソフトウェア モジュール、およびパスワードの機能を以下の表に示します。

この表には IT 管理者だけが設定して使用するパスワードも示してあります。その他すべてのパスワードは、通常のユーザーまたは管理者が設定できます。

ProtectTools パスワード	パスワードを設定する ProtectTools モジュール	機能
Computer Setup のセットアップ パスワード **注記**　別名：BIOS 管理者パスワード、F10 セットアップ パスワード、セキュリティ セットアップ パスワード	BIOS Configuration に IT 管理者が設定	Computer Setup ユーティリティへのアクセスを保護します。
電源投入時パスワード	BIOS Configuration	コンピュータの電源投入時、再起動時、または休止状態からの復帰時に、コンピュータのデータへのアクセスを保護します。
スマート カード管理者パスワード **注記**　別名：BIOS 管理者カード パスワード	Smart Card Security に IT 管理者が設定	スマート カードの電源投入時 (BIOS) の認証に使用されます。コンピュータの電源投入時、再起動時、または休止状態からの復帰時に、Computer Setup ユーティリティおよびコンピュータのデータへのアクセスを許可します。また、ユーザー カードまたは管理者カードを復元するためのリカバリ ファイルを作成することもできます。
スマート カード ユーザー パスワード **注記**　別名：BIOS ユーザー カード パスワード	Smart Card Security	スマート カードの電源投入時 (BIOS) の認証に使用されます。コンピュータの電源投入時、再起動時、または休止状態からの復帰時に、コンピュータのデータへのアクセスを許可します。
スマート カード PIN	Smart Card Security	スマート カードのデータへのアクセスを保護し、スマート カードのユーザーを認証します。また、電源投入時の認証に使用した場合、スマート カード PIN は、Computer Setup ユーティリティへのアクセスおよびコンピュータのデータへのアクセスを保護します。
スマート カード リカバリ ファイル パスワード	Smart Card Security	BIOS パスワードを含むリカバリ ファイルへのアクセスを保護します。
Java™ Card PIN	Java Card Security	Java Card データへのアクセスを保護し、Java Card のユーザーを認証します。また、電源投入時の認証に使用した場合、Java Card PIN は、Computer Setup ユーティリティへのアクセスおよびコンピュータのデータへのアクセスを保護します。
基本ユーザー キー パスワード	Embedded Security	暗号化によってセキュリティ保護された電子メール、ファイル、フォルダなどの Embedded Security の機能にアクセスするために使用されます。また、電源投入時の

ProtectTools パスワード	パスワードを設定する ProtectTools モジュール	機能
注記 別名：Embedded Security パスワード		認証に使用した場合は、コンピュータの電源投入時、再起動時、または休止状態からの復帰時に、コンピュータのデータへのアクセスを保護します。
緊急リカバリ トークン パスワード **注記** 別名：緊急リカバリ トークン キー パスワード	Embedded Security に IT 管理者が設定	内蔵セキュリティ チップのバックアップ ファイルである緊急リカバリ トークンへのアクセスを保護します。
所有者パスワード	Embedded Security に IT 管理者が設定	Embedded Security のすべての所有者機能に対する不正アクセスからシステムおよび TPM チップを保護します。
Credential Manager ログオン パスワード	Credential Manager	このパスワードには 2 つのオプションがあります。 • Microsoft Windows へのログオン後、Credential Manager にアクセスするための別個のログオンで使用できます。 • Windows ログオン プロセスの代わりに使用でき、Windows と Credential Manager への同時アクセスを可能にします。
Credential Manager リカバリ ファイル パスワード	Credential Manager に IT 管理者が設定	Credential Manager リカバリ ファイルへのアクセスを保護します。
Windows ログオン パスワード	Windows コントロール パネル	手動ログオンで使用するか、スマート カードに保存できます。

安全なパスワードの作成

パスワードを作成するときは、プログラムの指定に従う必要があります。一般に、強固なパスワードを作成し、パスワードが破られる可能性を少なくするためには、次のガイドラインを参考にしてください。

- 6 文字以上のパスワードを使用します。推奨は 8 文字以上です。
- パスワードに大文字と小文字を混ぜて使用します。
- 可能な限り、英数字、特殊文字、および句読点を混ぜて使用します。
- 単語の中の文字を特殊文字または数字に置き換えます。たとえば、I または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語の言葉を組み合わせます。
- 単語または句の途中に数字または特殊文字を挿入します。例：Mary2-2Cat45
- 辞書に載っている言葉をパスワードとして使用しないでください。
- 自分の名前や、その他の個人情報をパスワードとして使用しないでください。たとえば、誕生日、ペットの名前、母親の旧姓などは、たとえスペルを逆さにしたとしても、使用しないでください。
- パスワードは定期的に変更してください。増分する 1 文字か 2 文字だけを変更してもかまいません。
- パスワードをメモした場合、そのメモをコンピュータのそばの人目につく場所に保管しないでください。
- コンピュータ上のファイル (電子メールなど) にパスワードを保存しないでください。
- アカウントは共有しないでください。または、パスワードはだれにも教えないでください。

2 Smart Card Security for ProtectTools

Smart Card Security for ProtectTools では、別売のスマート カード リーダーを搭載したコンピュータで、スマート カードのセットアップと設定を管理します。

Smart Card Security を使用して、以下の操作を実行できます。

- スマート カード セキュリティ機能へのアクセス。
- スマート カードを初期化して、Credential Manager for ProtectTools などの他の ProtectTools モジュールで使用できるようにする。
- Computer Setup ユーティリティを操作して、電源投入時環境でのスマート カード認証を有効にし、管理者とユーザーに対して別々のスマート カードを設定する。これにより、ユーザーがオペレーティング システムをロードするには、スマート カードを挿入し、オプションで PIN を入力する必要があります。
- スマート カードのユーザーを認証するために使用されるパスワードの設定と変更。
- スマート カードに保存されるスマート カード BIOS パスワードのバックアップと復元。

スマート カードの初期化

スマート カードは、使用する前に初期化する必要があります。

スマート カードを初期化するには、次の手順を行います。

1. リーダーにスマート カードを挿入します。
2. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
3. 左側のペインで、**[Smart Card Security]** を選択し、**[Smart Card]** (スマート カード) を選択します。
4. 右側のペインで、**[Initialize]** (初期化) をクリックします。
5. **[Initialize the smart card]** (スマート カードの初期化) ダイアログ ボックスで、最初のボックスに名前を入力します。
6. スマート カード PIN を適切なボックスに設定し、確認します。PIN コードは 4 ～ 8 文字の数字でなければなりません。

注意 コンピュータにアクセスできなくなることを避けるために、スマート カード PIN を忘れないでください。スマート カード PIN を忘れた場合、コンピュータの操作が不可能になることがあります。スマート カード PIN を 5 回以内に正しく入力しない限り、スマート カードはロックされ、使用できなくなります この試行回数は、正しい PIN の入力後にリセットされます。

7. 初期化を完了するには、**[OK]** をクリックします。

スマート カード BIOS セキュリティ モード

スマート カード BIOS セキュリティを有効にすると、コンピュータを起動するにはスマート カードが必要になります。

スマート カード BIOS セキュリティ モードを有効にする手順は、次のとおりです。

1. BIOS Configuration でスマート カードの電源投入時認証サポートを有効にします。第 5 章「BIOS Configuration for ProtectTools」の「スマート カードまたは Java Card の電源投入時認証サポートの有効化と無効化」を参照してください。

注記 このオプションを有効にすると、電源投入時認証でスマート カードを使用できます。スマート カード BIOS セキュリティ モードは、スマート カードの電源投入時認証サポートを有効にするまでは使用できません。

2. Smart Card Security でスマート カード BIOS セキュリティ モードを有効にします。この章の後半の「スマート カード BIOS セキュリティ モードの有効化とスマート カード管理者パスワードの設定」を参照してください。

3. スマート カード管理者パスワードを設定します。

注記 スマート カード BIOS セキュリティ モードを有効にする処理の一部として、スマート カード管理者パスワードを設定します。

スマート カード管理者パスワードは、Computer Setup セットアップ パスワードと同じではありません。スマート カード管理者パスワードは、スマート カードを識別する目的でコンピュータに関連付け、以下の操作を可能にします。

- コンピュータの電源投入後、Computer Setup またはコンピュータのデータにアクセスする。
- 管理者用およびユーザー用の新しいスマート カードを作成する。
- ユーザー用または管理者用のスマート カードを復元するためのリカバリ ファイルを作成する。

スマート カード BIOS セキュリティ モードの有効化とスマート カード管理者パスワードの設定

スマート カード BIOS セキュリティ モードを有効にしてスマート カード管理者パスワードを設定するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[BIOS]** を選択します。
3. 右側のペインで、[BIOS Security Mode] (BIOS セキュリティ モード) の **[Enable]** (有効化) をクリックします。
4. **[Next]** (次へ) をクリックします。
5. Computer Setup のセットアップ パスワードを入力し、**[Next]** (次へ) をクリックします。
6. 新しい管理者スマート カードを挿入し、画面の説明に沿って操作します。画面の説明は一定ではなく、以下のタスクが含まれることがあります。
   - スマート カードの初期化。詳しくは、「スマート カードの初期化」を参照してください。
   - スマート カード管理者パスワードの設定。詳しくは、「管理者またはユーザー カード パスワードの保存」を参照してください。
   - リカバリ ファイルの作成。詳しくは、「リカバリ ファイルの作成」を参照してください。

スマート カード BIOS セキュリティ モードの無効化

スマート カード BIOS セキュリティ モードを無効にすると、スマート カードの管理者パスワードとユーザー パスワードが無効になり、スマート カードを使用しなくてもコンピュータにアクセスできるようになります。

注記 スマート カード BIOS セキュリティ モードが有効になっている場合は、[Smart Card Security BIOS] ページのボタンが [Disable] (無効化) に変わります。

スマート カード セキュリティを無効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[BIOS]** を選択します。
3. 右側のペインで、**[BIOS Security Mode]** (BIOS セキュリティ モード) の **[Disable]** (無効化) をクリックします。
4. 現在のスマート カード管理者パスワードが設定されているカードを挿入し、**[Next]** (次へ) をクリックします。
5. メッセージに従ってスマート カード PIN を入力し、**[Finish]** (終了) をクリックします

スマート カード管理者パスワードの変更

スマート カード BIOS セキュリティ モードを有効にする処理の一部として、スマート カード管理者パスワードを設定します。スマート カード管理者パスワードは、設定した後に変更できます。スマート カード管理者パスワードについて詳しくは、この章の前半の「スマート カード BIOS セキュリティ モード」を参照してください。

注記　以下の手順では、スマート カードと Computer Setup に記録されるスマート カード管理者パスワードを更新します。

スマート カード管理者パスワードを変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[BIOS]** を選択します。
3. 右側のペインで、**[BIOS administrator card]** (BIOS 管理者カード) の横にある **[BIOS Security Mode]** (BIOS セキュリティ モード) の **[Change]** (変更) をクリックします。
4. スマート カード PIN を入力し、**[Next]** (次へ) をクリックします。
5. 新しい管理者カードを挿入し、**[Next]** (次へ) をクリックします。
6. スマート カード PIN を入力し、**[Finish]** (終了) をクリックします。

スマート カード ユーザー パスワードの設定と変更

スマート カード ユーザー パスワードを設定または変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[BIOS]** を選択します。
3. 右側のペインで、**[BIOS user card]** (BIOS ユーザー カード) の横にある **[BIOS Security Mode]** (BIOS セキュリティ モード) の **[Set]** (設定) をクリックします。

注記　Computer Setup でユーザー パスワードが既に設定されている場合は、**[Change]** (変更) ボタンをクリックします。

4. スマート カード PIN を入力し、**[Next]** (次へ) をクリックします。
5. 新しいユーザー カードを挿入し、**[Next]** (次へ) をクリックします。
   - カードに既にユーザー パスワードが設定されている場合は、**[Finish]** (終了) ダイアログ ボックスが表示されます。手順 6 ～ 8 を飛ばして手順 9 に進んでください。
   - カードにパスワードが設定されていない場合は、BIOS パスワード ウィザードが開きます。
6. BIOS パスワード ウィザードでは、以下のいずれかを実行できます。
   - パスワードを手動で入力する。
   - 32 バイトのパスワードをランダムに生成する。

注記　既知のパスワードを使用すると、リカバリ ファイルを使用せずに複製カードを作成できます。ランダム パスワードを生成すると、安全性が高まります。ただし、バックアップ カードを作成するにはリカバリ ファイルが必要です。

7. 起動時にスマート カード PIN の入力が必要な場合は、**[Boot Requirements]** (ブート要件) で該当するチェック ボックスをオンにします。

注記　起動時にスマート カード PIN の入力が不要な場合は、このチェック ボックスをオフにします。

8. スマート カード PIN を入力し、**[OK]** をクリックします。リカバリ ファイルを作成するメッセージが表示されます。

注記　リカバリ ディスクを作成することを強くお勧めします。詳しくは、この章の後半の「リカバリ ファイルの作成」を参照してください。

9. **[Finish]** (終了) ダイアログ ボックスにスマート カード PIN を入力し、**[Finish]** (終了) をクリックします。

管理者またはユーザー カード パスワードの保存

バックアップ カードを作成する時点で管理者パスワードが既に設定されている場合は、そのパスワードを新しいカードに保存できます。

注意　以下の手順では、スマート カードに保存されるパスワードのみを更新し、Computer Setup に記録されるパスワードは更新しません。新しいカードを使用してコンピュータにアクセスすることはできません。

管理者またはユーザーのカード パスワードを保存するには、次の手順を行います。

1. リーダーにスマート カードを挿入します。
2. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
3. 左側のペインで、**[Smart Card Security]** を選択し、**[BIOS]** を選択します。
4. 右側のペインで、**[BIOS Password on Smart Card]** (スマート カードの BIOS パスワード) の **[Store]** (保存) をクリックします。
5. BIOS パスワード ウィザードでは、以下のいずれかを実行できます。
   - パスワードを手動で入力する。
   - 32 バイトのパスワードをランダムに生成する。

   注記　既知のパスワードを使用すると、リカバリ ファイルを使用せずに複製カードを作成できます。ランダム パスワードを生成すると、安全性が高まります。ただし、バックアップ カードを作成するにはリカバリ ファイルが必要です。
6. カードの種類として、**[Access Privilege]** (アクセス権限) の **[Administrator]** (管理者) または **[User]** (ユーザー) のいずれかをクリックします。
7. 起動時にスマート カード PIN の入力が必要な場合は、**[Boot Requirements]** (ブート要件) で該当するチェック ボックスをオンにします。

   注記　起動時にスマート カード PIN の入力が不要な場合は、このチェック ボックスをオフにします。
8. スマート カード PIN を入力し、**[OK]** をクリックします。
9. **[Finish]** (終了) ダイアログ ボックスに再度スマート カード PIN を入力し、**[Finish]** (終了) をクリックします。

   リカバリ ファイルを作成するメッセージが表示されます。

   注記　スマート カード リカバリ ディスクを作成することを強くお勧めします。詳しくは、この章の後半の「リカバリ ファイルの作成」を参照してください。

全般的なタスク

BIOS スマート カード設定の更新

コンピュータの起動時にスマート カード PIN を要求するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[BIOS]** を選択します。
3. 右側のペインで、**[Smart Card BIOS Password Properties]** (スマート カード BIOS パスワードのプロパティ) の **[Settings]** (設定) をクリックします。
4. 再起動時に PIN を要求するには、チェック ボックスをオンにします。

   注記　この要件を除去するには、チェック ボックスをオフにします。

5. スマート カード PIN を入力し、**[OK]** をクリックします。

スマート カード リーダーの選択

スマート カードを使用する前に、Smart Card Security で正しいスマート カード リーダーが選択されていることを確認してください。Smart Card Security で正しいスマート カード リーダーが選択されていない場合、一部の機能が使用できなかったり、正しく表示されなかったりすることがあります。

スマート カード リーダーを選択するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[General]** (全般) を選択します。
3. 右側のペインで、**[Smart Card Reader]** (スマート カード リーダー) から正しいリーダーを選択します。
4. リーダーにスマート カードを挿入します。リーダー情報が自動的に更新されます。

スマート カード PIN の変更

スマート カード PIN を変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[Smart Card]** (スマート カード) を選択します。
3. 右側のペインで、**[Change PIN]** (PIN の変更) の **[Change PIN]** (PIN の変更) をクリックします。
4. 現在のスマート カード PIN を入力します。
5. 新しい PIN を設定して確認します。
6. 確認ダイアログ ボックスで **[OK]** をクリックします。

スマート カードのバックアップと復元

スマート カードを初期化して使用できる状態になった後、スマート カード リカバリ ファイルを作成することを強くお勧めします。リカバリ ファイルを使用すると、あるスマート カードのデータを別のスマート カードに転送できます。また、このファイルは、オリジナルのスマート カードをバックアップするため、またはスマート カードの紛失や盗難の場合にデータを復元するためにも使用できます。

注意　更新されたスマート カードの情報と保管しているリカバリ ファイルが一致しなくなることを避けるために、直ちに新しいリカバリ ファイルを作成し、安全な場所に保管してください。バックアップ スマート カードがある場合は、新しいリカバリ ファイルをバックアップ スマート カード上に復元して、バック アップスマート カードの情報も必ず更新してください。

リカバリ ファイルの作成

リカバリ ファイルを作成するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[Smart Card]** (スマート カード) を選択します。
3. 右側のペインで、**[Recovery]** (リカバリ) の **[Create]** (作成) をクリックします。
4. スマート カード PIN を入力し、**[OK]** をクリックします。
5. **[Filename]** (ファイル名) ボックスにファイルのパスとファイル名を入力します。

   注意　コンピュータにアクセスできなくなる事態を避けるために、コンピュータのハード ドライブ上にリカバリ ファイルを保存しないでください。スマート カードがないとリカバリ ファイルにアクセスできなくなります。また、ハード ドライブに保存されたリカバリ ファイルは他のユーザーもアクセスできるので、セキュリティ上のリスクが生じます。

6. リカバリ ファイル パスワードを設定して確認し、**[OK]** をクリックします。

注意　スマート カード リカバリ ファイルのデータが失われないように、リカバリ ファイル パスワードを忘れないようにしてください。パスワードを忘れた場合は、リカバリ ファイルからカードを再作成できません。

スマート カードのデータの復元

リカバリ ファイルからスマート カード データを復元できます。これは、カードの紛失または盗難が発生した場合、またはバックアップ スマート カードを作成する場合に特に便利です。前のデータが保存されているカードを使用すると、データは上書きされます。

開始するには、以下のものが必要です。

- Smart Card Security ソフトウェアがインストールされているコンピュータへのアクセス権
- スマート カード リカバリ ファイル
- スマート カード リカバリ ファイル パスワード
- スマート カード

スマート カードを復元するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Smart Card Security]** を選択し、**[Smart Card]** (スマート カード) を選択します。
3. スマート カード リカバリ ファイルが保存されているフロッピー ディスクまたはその他のメディアを挿入します。
4. リーダーにスマート カードを挿入します。カードが初期化されていない場合は、初期化を実行するメッセージが表示されます。スマート カードを初期化する手順については、この章の前半の「スマート カードの初期化」を参照してください。
5. 右側のペインで、**[Recovery]** (リカバリ) の **[Restore]** (復元) をクリックします。
6. 正しいリカバリ ファイル名を選択していることを確認し、リカバリ ファイル パスワードを入力します。
7. スマート カード PIN を入力します。
8. **[OK]** をクリックします。オリジナルのスマート カードの内容が新しい スマート カードに復元されます。

バックアップ スマート カードの作成

バックアップの目的のために、スマート カードの複製を作成することを強くお勧めします。バックアップ カードは、2 つの方法で作成できます。どちらを使用するかは、スマート カード パスワードを手動で作成するか、ランダムに生成するかによって決まります。

ランダムに生成されるスマート カード パスワードを使用して代替スマート カードを作成するには、次の手順を行います。

▲ リーダーにスマート カードを挿入し、適切なリカバリ ファイルを読み込みます。詳しくは、この章の前半の「スマート カードのデータの復元」を参照してください。

手動で作成するスマート カード パスワードを使用して代替スマート カードを作成するには、次の手順を行います。

1. 新しいスマート カードを初期化します。詳しくは、この章の前半の「スマート カードの初期化」を参照してください。
2. 新しいスマート カードに、管理者またはユーザー カード パスワードを保存します。詳しくは、この章の前半の「管理者またはユーザー カード パスワードの保存」を参照してください。

3 Java Card Security for ProtectTools

Java Card Security for ProtectTools では、別売のスマート カード リーダーを取り付けたコンピュータでの Java Card のセットアップと設定を管理します。

Java Card Security を使用して、以下の操作を実行できます。

- Java Card セキュリティ機能へのアクセス。
- Computer Setup ユーティリティを操作して、電源投入時環境での Java Card 認証を有効にし、管理者とユーザーに対して別々の Java Card を設定する。これにより、ユーザーがオペレーティング システムをロードするには、Java Card を挿入し、PIN を入力する必要があります。
- Java Card ユーザーの認証に使用される PIN の設定と変更。
- Java Card に保存される電源投入時認証データのバックアップと復元。

全般的なタスク

[General] (全般) ページでは、以下のタスクを実行できます。

- Java Card PIN の変更
- スマート カード リーダーの選択

注記　スマート カード リーダーでは、Java Card とスマート カードの両方を使用できます。この機能は、コンピュータに複数のスマート カード リーダーがある場合にのみ、使用可能です。

Java Card PIN の変更

Java Card PIN を変更するには、次の手順を行います。

注記　Java Card PIN は 4 ～ 8 文字の数字でなければなりません。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[General]** (全般) を選択します。
3. スマート カード リーダーに Java Card (既存の PIN が設定されたもの) を挿入します。
4. 右側のペインで、**[Change]** (変更) をクリックします。
5. **[Change PIN]** (PIN の変更) ダイアログ ボックスで、**[Current PIN]** (現在の PIN) ボックスに現在の PIN を入力します。
6. **[New PIN]** (新しい PIN) ボックスに新しい PIN を入力し、**[Confirm New PIN]** (新しい PIN の確認) ボックスに PIN を再度入力します。
7. **[OK]** をクリックします。

スマート カード リーダーの選択

Java Card を使用する前に、Java Card Security で正しいスマート カード リーダーが選択されていることを確認してください。Java Card Security で正しいスマート カード リーダーが選択されていない場合、一部の機能が使用できなかったり、正しく表示されなかったりすることがあります。

スマート カード リーダーを選択するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[General]** (全般) を選択します。
3. スマート カード リーダーに Java Card を挿入します。
4. 右側のペインで、**[Smart Card Reader]** (スマート カード リーダー) から正しいリーダーを選択します。

高度なタスク (管理者専用)

[Advanced] (詳細) ページでは、以下のタスクを実行できます。

- Java Card PIN の割り当て
- Java Card への名前の割り当て
- 電源投入時認証の設定
- Java Card のバックアップと復元

注記　[Advanced] (詳細) ページにアクセスするには、Computer Setup のセットアップ パスワードが必要です。

Java Card PIN の割り当て

Java Card を電源投入時の認証に使用するは、Java Card に PIN を割り当てる必要があります。

Java Card に PIN を割り当てるには、次の手順を行います。

注記　Java Card PIN は 4 ～ 8 文字の数字でなければなりません。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[General]** (全般) を選択します。
3. スマート カード リーダーに新しい Java Card を挿入します。
4. **[Change PIN]** (PIN の変更) ダイアログ ボックスが表示されたら、**[New PIN]** (新しい PIN) ボックスに新しい PIN を入力し、**[Confirm New PIN]** (新しい PIN の確認) ボックスにその PIN を再度入力します。
5. **[OK]** をクリックします。

Java Card への名前の割り当て

Java Card を電源投入時の認証に使用するには、Java Card に名前を割り当てる必要があります。

Java Card に名前を割り当てるには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[Advanced]** (詳細) を選択します。
3. **[Setup Password]** (セットアップ パスワード) ダイアログ ボックスが表示されたら、Computer Setup のセットアップ パスワードを入力し、**[OK]** をクリックします。
4. スマート カード リーダーに Java Card を挿入します。

注記　このカードに PIN をまだ割り当てていない場合は、[Change PIN] (PIN の変更) ダイアログ ボックスが開き、新しい PIN を入力できます。

5. 右側のペインで、**[Java Card]** 名の **[Change]** (変更) をクリックします。
6. **[Name]** (名前) ボックスに Java Card の名前を入力します。
7. **[PIN]** ボックスに現在の Java Card PIN を入力します。
8. **[OK]** をクリックします。

電源投入時認証の設定

電源投入時の認証を有効にすると、コンピュータを起動するために Java Card が必要になります。

Java Card の電源投入時認証を有効にする手順は、次のとおりです。

1. BIOS Configuration または Computer Setup で Java Card の電源投入時認証サポートを有効にします。第 5 章「BIOS Configuration for ProtectTools」の「スマート カードまたは Java Card の電源投入時認証サポートの有効化と無効化」を参照してください。
2. Java Card Security で Java Card の電源投入時認証を有効にします。この章の後半の「Java Card の電源投入時認証の有効化と管理者 Java Card の作成」を参照してください。
3. 管理者 Java Card を作成し、有効にします。

Java Card の電源投入時認証の有効化と管理者 Java Card の作成

Java Card の電源投入時認証を有効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[Advanced]** (詳細) を選択します。
3. **[Computer Setup Password]** (コンピュータ セットアップ パスワード) ダイアログ ボックスが表示されたら、Computer Setup のセットアップ パスワードを入力し、**[OK]** をクリックします。
4. スマート カード リーダーに Java Card を挿入します。

   注記　このカードに PIN をまだ割り当てていない場合は、**[Change PIN]** (PIN の変更) ダイアログ ボックスが開き、新しい PIN を入力できます。

5. 右側のペインで、**[Power-on authentication]** (電源投入時認証) の **[Enable]** (有効化) チェック ボックスをクリックします。
6. DriveLock を有効にしていない場合は、Java Card PIN を入力し、**[OK]** をクリックします。

   - または -

   DriveLock を有効にしている場合：

   a. **[Make Java card identity unique]** (Java Card ID を一意にする) を選択します。

      - または -

      [Make the Java card identity the same as the DriveLock password] (Java Card ID を DriveLock パスワードと同じにする) を選択します。

      注記　コンピュータに対して DriveLock が有効になっている場合は、Java Card ID を DriveLock ユーザー パスワードと同じに設定できます。このように設定すると、コンピュータの起動時に Java Card だけを使用して DriveLock と Java Card の両方を検証できます。

   b. 必要に応じて、**[DriveLock password]** (DriveLock パスワード) ボックスに DriveLock ユーザー パスワードを入力し、**[Confirm password]** (パスワードの確認) ボックスに再度入力します。

   c. Java Card PIN を入力します。

   d. **[OK]** をクリックします。

7. リカバリ ファイルを作成するメッセージが表示された場合は、「リカバリ ファイルの作成」を参照してください。または、**[Cancel]** (キャンセル) をクリックして、リカバリ ファイルを後で作成することもできます。

ユーザー Java Card の作成

注記　ユーザー Java Card を作成するためには、電源投入時認証と管理者カードを設定する必要があります。

ユーザー Java Card を作成するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[Advanced]** (詳細) を選択します。
3. **[Setup Password]** (セットアップ パスワード) ダイアログ ボックスが表示されたら、Computer Setup のセットアップ パスワードを入力し、**[OK]** をクリックします。
4. ユーザー カードとして使用する Java Card を挿入します。
5. 右側のペインで、**[Power-on authentication]** (電源投入時認証) の **[User card identity]** (ユーザー カード ID) の横にある **[Create]** (作成) をクリックします。
6. ユーザー Java Card の PIN を入力し、[OK] をクリックします。

Java Card の電源投入時認証の無効化

Java Card の電源投入時認証を無効にすると、コンピュータにアクセスするために Java Card は必要なくなります。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[Advanced]** (詳細) を選択します。
3. **[Setup Password]** (セットアップ パスワード) ダイアログ ボックスが表示されたら、Computer Setup のセットアップ パスワードを入力し、**[OK]** をクリックします。
4. Java Card を挿入し、PIN を入力して、**[OK]** をクリックします。
5. 右側のペインで、**[Power-on authentication]** (電源投入時認証) の **[Enable]** (有効化) チェック ボックスをオフにします。

Java Card のバックアップと復元

Java Card に電源投入時認証 ID を割り当てた後、Java Card リカバリ ファイルを作成することを強く お勧めします。リカバリ ファイルを使用すると、ある Java Card の Java Card 電源投入時認証 ID データを別の Java Card に転送できます。また、このファイルは、オリジナルの Java Card をバックアップするため、または Java Card の紛失や盗難の場合にデータを復元するためにも使用できます。

注意 更新された Java Card の情報と保管しているリカバリ ファイルが一致しなくなることを避けるために、直ちにリムーバブル メディアに新しいリカバリ ファイルを作成し、安全な場所に保管してください。バックアップ Java Card がある場合は、新しいリカバリ ファイルをバックアップ Java Card 上に復元して、バックアップ Java Card の情報も必ず更新してください。

リカバリ ファイルの作成

リカバリ ファイルを作成するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[Advanced]** (詳細) を選択します。
3. **[Setup Password]** (セットアップ パスワード) ダイアログ ボックスが表示されたら、Computer Setup のセットアップ パスワードを入力し、**[OK]** をクリックします。
4. 右側のペインで、**[Recovery]** (リカバリ) の **[Create]** (作成) をクリックします。
5. **[Filename]** (ファイル名) ボックスにファイルのパスとファイル名を入力します。

   注意 コンピュータにアクセスできなくなる事態を避けるために、コンピュータのハードドライブ上にリカバリ ファイルを保存しないでください。Java Card がないとリカバリ ファイルにアクセスできなくなります。また、ハード ドライブに保存されたリカバリ ファイルは他のユーザーもアクセスできるので、セキュリティ上のリスクが生じます。

6. **[Recovery file password]** (リカバリ ファイル パスワード) ボックスにリカバリ ファイルのパスワードを入力し、**[Confirm password]** (パスワードの確認) ボックスに再度入力します。
7. Java Card PIN を入力し、**[OK]** をクリックします。

注意 Java Card リカバリ ファイルのデータが失われないように、リカバリ ファイル パスワードを忘れないようにしてください。パスワードを忘れた場合は、リカバリ ファイルからカードを再作成できません。

Java Card データの復元

リカバリ ファイルから Java Card データを復元できます。これは、カードの紛失または盗難が発生した場合、またはバックアップ Java Card を作成する場合に特に便利です。前のデータが保存されているカードを使用すると、データは上書きされます。

開始するには、以下のものが必要です。

- Java Card Security ソフトウェアがインストールされているコンピュータへのアクセス権
- Java Card リカバリ ファイル
- Java Card リカバリ ファイル パスワード
- Java Card

Java Card を復元するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Java Card Security]** (Java Card セキュリティ) を選択し、**[Advanced]** (詳細) を選択します。
3. **[Setup Password]** (セットアップ パスワード) ダイアログ ボックスが表示されたら、Computer Setup のセットアップ パスワードを入力し、**[OK]** をクリックします。
4. Java Card リカバリ ファイルが保存されているフロッピー ディスクまたはその他のメディアを挿入します。
5. リーダーに Java Card を挿入します。カードに PIN が割り当てられていない場合は、PIN を作成するメッセージが表示されます。Java Card に PIN を割り当てる手順については、この章の前半の「Java Card PIN の割り当て」を参照してください。
6. 右側のペインで、**[Recovery]** (リカバリ) の **[Restore]** (復元) をクリックします。
7. 正しいリカバリ ファイル名を選択していることを確認し、リカバリ ファイル パスワードを入力します。
8. Java Card PIN を入力します。
9. **[OK]** をクリックします。

   オリジナルの Java Card の内容が新しい Java Card に復元されます。

バックアップ Java Card の作成

バックアップの目的のために、Java Card の複製を作成することを強くお勧めします。

交換 Java Card を作成するには、次の手順を行います。

▲ リーダーに Java Card を挿入し、適切なリカバリ ファイルを読み込みます。詳しくは、この章の前半の「Java Card データの復元」を参照してください。

4 Embedded Security for ProtectTools

注記 Embedded Security for ProtectTools を使用するには、トラステッド プラットフォーム モジュール (TPM) 内蔵セキュリティ チップがコンピュータに搭載されている必要があります。

Embedded Security for ProtectTools は、ユーザー データや資格情報への不正アクセスを防止します。このソフトウェア モジュールには、以下のセキュリティ機能があります。

- Enhanced Microsoft Encryption File System (EFS) ファイルとフォルダの暗号化
- ユーザー データを保護するためのパーソナル セキュア ドライブ (PSD) の作成
- キー階層のバックアップや復元などのデータ管理機能
- Embedded Security ソフトウェア使用時にデジタル証明書の保護操作を行うためのサードパーティ アプリケーション (Microsoft Outlook や Internet Explorer など) のサポート

TPM 内蔵セキュリティ チップは、他の ProtectTools セキュリティ マネージャのセキュリティ機能を拡張し、実現します。たとえば、Credential Manager for ProtectTools は、ユーザーが Windows にログインしたときに、認証要素として内蔵チップを使用できます。一部のモデルでは、TPM 内蔵セキュリティ チップによって、BIOS Configuration for ProtectTools からアクセスする拡張 BIOS セキュリティ機能も実現されます。

セットアップ手順

注意　セキュリティ上のリスクを軽減するために、内蔵セキュリティ チップは IT 管理者が直ちに初期化するように強くお勧めします。内蔵セキュリティ チップを初期化しないと、権限のないユーザー、コンピュータ ワーム、またはウイルスがコンピュータの所有者の権限を取得し、緊急リカバリ アーカイブの取り扱いやユーザー アクセス権の設定などの所有者タスクの制御権を取得する可能性があります。

内蔵セキュリティ チップを有効にして初期化するには、以下の 2 つのセクションで説明する手順に従います。

内蔵セキュリティ チップの有効化

Computer Setup ユーティリティで内蔵セキュリティ チップを有効にする必要があります。この手順は、BIOS Configuration for ProtectTools では実行できません。

内蔵セキュリティ チップを有効にするには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 管理者パスワードが設定されていない場合は、矢印キーを使用して **[Security]** (セキュリティ) **[> Setup password]** (パスワードの設定) の順に選択し、Enter キーを押します。
3. **[New password]** (新しいパスワード) と **[Verify new password]** (新しいパスワードの確認) にパスワードを入力し、F10 キーを押します。
4. **[Security]** (セキュリティ) メニューで、矢印キーを使用して **[TPM Embedded Security]** を選択し、Enter キーを押します。
5. **[Embedded Security]** で、デバイスが非表示になっている場合は **[Available]** (使用可能) を選択します。
6. **[Embedded security device state]** (Embedded Security デバイスの状態) を選択し、**[Enable]** (有効化) に変更します。
7. Embedded Security 設定の変更を確定するには、F10 キーを押します。
8. 設定を保存して Computer Setup を終了するには、矢印キーを使用して **[File]** (ファイル) **[> Save Changes and Exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

内蔵セキュリティ チップの初期化

Embedded Security の初期化プロセスでは、以下の操作を行います。

- 内蔵セキュリティ チップでのすべての所有者機能へのアクセスを保護する、内蔵セキュリティ チップの所有者パスワードを設定します。
- すべてのユーザーの基本ユーザー キーの再暗号化を可能にする、保護された記憶域である緊急リカバリ アーカイブをセットアップします。

内蔵セキュリティ チップを初期化するには、次の手順を行います。

1. タスクバーの右端の通知領域にある ProtectTools Security Manager アイコンを右クリックし、**[Embedded Security Initialization]** (Embedded Security の初期化) をクリックします。

   ProtectTools Embedded Security 初期化ウィザードが開きます。

2. **[Next]** (次へ) をクリックします。
3. 所有者パスワードを設定して確認し、**[Next]** (次へ) をクリックします。

   [Setup Emergency Recovery] (緊急リカバリのセットアップ) ダイアログ ボックスが開きます。

4. **[Next]** (次へ) をクリックしてデフォルトのリカバリ アーカイブの場所をそのまま使用するか、**[Browse]** (参照) をクリックして別の場所を選択し、**[Next]** (次へ) をクリックします。
5. 緊急リカバリ トークン パスワードを設定して確認し、**[Next]** (次へ) をクリックします。
6. **[Browse]** (参照) をクリックして緊急リカバリ アーカイブの場所を選択し、**[Next]** (次へ) をクリックします。
7. [Summary] (概要) ページで **[Next]** (次へ) をクリックします。
   - この時点で基本ユーザー アカウントをセットアップしない場合は、**[Start the Embedded Security User Initialization Wizard]** (Embedded Security ユーザー初期化ウィザードの起動) チェック ボックスをオフにし、**[Finish]** (終了) をクリックします。次のセクションの指示に従ってウィザードを手動で起動し、いつでも基本ユーザー アカウントをセットアップできます。
   - 基本ユーザー アカウントをセットアップする場合は、**[Start the Embedded Security User Initialization Wizard]** (Embedded Security ユーザー初期化ウィザード) チェック ボックスをオンにし、**[Finish]** (終了) をクリックします。Embedded Security ユーザー初期化ウィザードが開きます。詳しくは、次のセクションの手順を参照してください。

基本ユーザー アカウントのセットアップ

Embedded Security での基本ユーザー アカウントのセットアップでは、次の操作を行います。

- 暗号化された情報を保護する基本ユーザー キーを作成し、基本ユーザー キーを保護する基本ユーザー キー パスワードを設定します。
- 暗号化されたファイルとフォルダを保存するためのパーソナル セキュア ドライブ (PSD) をセットアップします。

注意　基本ユーザー キー パスワードは、厳重に管理してください。暗号化された情報へのアクセスまたは暗号化された情報の回復には、このパスワードが必要です。

基本ユーザー アカウントをセットアップし、ユーザー セキュリティ機能を有効にするには、次の手順を行います。

1. Embedded Security ユーザー初期化ウィザードが開いていない場合は、**[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Embedded Security]** を選択し、**[User Settings]** (ユーザー設定) を選択します。
3. 右側のペインで、**[Embedded Security Features]** (Embedded Security の機能) の **[Configure]** (設定) をクリックします。

   Embedded Security ユーザー初期化ウィザードが開きます。
4. **[Next]** (次へ) をクリックします。
5. 基本ユーザー キー パスワードを設定して確認し、**[Next]** (次へ) をクリックします。
6. **[Next]** (次へ) をクリックして設定を確認します
7. 目的のセキュリティ機能を選択し、**[Next]** (次へ) をクリックします。
8. **[Next]** (次へ) を再度クリックします。

   注記　セキュリティで保護された電子メールを使用するには、その前に、Embedded Security で作成したデジタル証明書を使用して電子メール クライアントを設定する必要があります。デジタル証明書がない場合は、証明機関から取得する必要があります。電子メールの設定とデジタル証明書の取得については、電子メール クライアントのヘルプを参照してください。
9. 複数の暗号証明書が存在する場合は、適切な証明書を選択し、**[Next]** (次へ) をクリックします。
10. PSD 用のドライブ文字とラベルを選択し、**[Next]** (次へ) をクリックします。
11. PSD のサイズと場所を選択し、**[Next]** (次へ) をクリックします。
12. [Summary] (概要) ページで **[Next]** (次へ) をクリックします。
13. **[Finish]** (終了) をクリックします。

全般的なタスク

基本ユーザー アカウントをセットアップした後、以下のタスクを実行できます。

- ファイルとフォルダの暗号化。
- 暗号化された電子メールの送受信。

パーソナル セキュア ドライブの使用

PSD をセットアップした後、次回のログオン時に基本ユーザー キー パスワードの入力を求められます。基本ユーザー キー パスワードを正しく入力すると、Windows エクスプローラから PSD に直接アクセスできます。

ファイルとフォルダの暗号化

Windows XP Professional で暗号化ファイルを扱うときは、以下の規則を考慮してください。

- NTFS パーティションのファイルとフォルダだけを暗号化できます。FAT パーティションのファイルとフォルダは暗号化できません。
- システム ファイルと圧縮ファイルは暗号化できません。また、暗号化されたファイルは圧縮できません。
- 一時フォルダはハッカーの攻撃対象になる可能性があるので、暗号化します。
- ファイルまたはフォルダを初めて暗号化したときに、回復ポリシーが自動的にセットアップされます。このポリシーによって、暗号証明書と秘密鍵をなくした場合に回復エージェントを使用して情報を復号化できます。

ファイルとフォルダを暗号化するには、次の手順を行います。

1. 暗号化するファイルまたはフォルダを右クリックします。
2. **[Encrypt]** (暗号化) をクリックします。
3. 以下のオプションのいずれかを選択します。
   - **[Apply changes to this folder only]** (このフォルダにのみ変更を適用する)
   - **[Apply changes to this folder, subfolders, and files]** (このフォルダ、サブフォルダ、およびファイルに変更を適用する)
4. **[OK]** をクリックします。

暗号化された電子メールの送受信

Embedded Security を使用して暗号化された電子メールを送受信できますが、手順は、電子メールにアクセスするために使用するプログラムによって異なります。詳しくは、Embedded Security と電子メールのヘルプを参照してください。

基本ユーザー キー パスワードの変更

基本ユーザー キー パスワードを変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Embedded Security]** を選択し、**[User Settings]** (ユーザー設定) を選択します。
3. 右側のペインで、**[Basic User Key password]** (基本ユーザー キー パスワード) の **[Change]** (変更) をクリックします。
4. 古いパスワードを入力し、新しいパスワードを設定して確認します。
5. **[OK]** をクリックします。

高度なタスク

バックアップと復元

Embedded Security のバックアップ機能は、緊急時に復元する認証情報を含むアーカイブを作成する機能です。

バックアップ ファイルの作成

バックアップ ファイルを作成するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Embedded Security]** を選択し、**[Backup]** (バックアップ) を選択します。
3. 右側のペインで、**[Backup]** (バックアップ) をクリックします。
4. **[Browse]** (参照) をクリックして、バックアップ ファイルの保存場所を選択します。
5. バックアップ情報に緊急リカバリ アーカイブを追加するかどうかを選択します。
6. **[Next]** (次へ) をクリックします。
7. **[Finish]** (終了) をクリックします。

バックアップ ファイルからの認証の復元

バックアップ ファイルからデータを復元するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Embedded Security]** を選択し、**[Backup]** (バックアップ) を選択します。
3. 右側のペインで、**[Restore]** (復元) をクリックします。
4. **[Browse]** (参照) をクリックして、保存場所からバックアップ ファイルを選択します。
5. **[Next]** (次へ) をクリックします。
6. Embedded Security ユーザー初期化ウィザードを起動するかどうかを選択します。
   - 初期化ウィザードの起動を選択した場合は、[Finish] (終了) をクリックし、画面の説明に沿って初期化を完了します。詳しくは、この章の前半の「基本ユーザー アカウントのセットアップ」を参照してください。
   - Embedded Security ユーザー初期化ウィザードを起動しないことを選択した場合は、**[Finish]** (終了) をクリックします。

所有者パスワードの変更

所有者パスワードを変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Embedded Security]** を選択し、**[Advanced]** (詳細) を選択します。
3. 右側のペインで、**[Owner Password]** (所有者パスワード) の **[Change]** (変更) をクリックします。
4. 古い所有者パスワードを入力し、新しい所有者パスワードを設定して確認します。
5. **[OK]** をクリックします。

ユーザー パスワードの再設定

パスワードを忘れた場合は、パスワードの再設定方法を管理者に問い合わせてください。詳しくは、ヘルプを参照してください。

Embedded Security の有効化と無効化

セキュリティ機能を使用しないで作業する必要がある場合は、Embedded Security 機能を無効にできます。

Embedded Security 機能は、以下の異なる 2 つのレベルで有効または無効にできます。

- 一時的な無効化 - このオプションを指定すると、Embedded Security は、Windows の再起動時に自動的に再度有効になります。このオプションは、デフォルトですべてのユーザーが使用できるようになっています。
- 永続的な無効化 - このオプションを指定すると、Embedded Security を再度有効にするには所有者パスワードが必要です。このオプションは、管理者だけが使用できます。

Embedded Security の永続的な無効化

Embedded Security を永続的に無効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Embedded Security]** を選択し、**[Advanced]** (詳細) を選択します。
3. 右側のペインで、**[Embedded Security]** の **[Disable]** (無効化) をクリックします。
4. プロンプトで所有者パスワードを入力し、**[OK]** をクリックします。

永続的に無効にした Embedded Security の有効化

Embedded Security を永続的に無効にした後で有効化するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Embedded Security]** を選択し、**[Advanced]** (詳細) を選択します。
3. 右側のペインで、**[Embedded Security]** の **[Enable]** (有効化) をクリックします。
4. プロンプトで所有者パスワードを入力し、**[OK]** をクリックします。

移行ウィザードを使用したキーの移行

移行は、キーと証明書の管理、復元、および転送を可能にする高度なタスクです。

移行について詳しくは、Embedded Security のヘルプを参照してください。

5 BIOS Configuration for ProtectTools

BIOS Configuration for ProtectTools では、Computer Setup ユーティリティのセキュリティ設定および構成設定にアクセスできます。これにより、ユーザーは、Computer Setup によって管理されているシステム セキュリティ機能に Windows からアクセスできます。

BIOS Configuration を使用して、以下の操作を実行できます。

- 電源投入時パスワードと管理者パスワードの管理
- スマート カード パスワードや内蔵セキュリティ認証の有効化などのその他の電源投入時認証機能の設定
- CD-ROM ブートや複数のハードウェア ポートなどのハードウェア機能の有効化と無効化
- MultiBoot の有効化やブート順序の変更などを含むブート オプションの設定

注記 BIOS Configuration for ProtectTools の機能の大半は、Computer Setup でも使用できます。

全般的なタスク

BIOS Configuration を使用すると、起動時に F10 キーを押して Computer Setup を開くことによってのみアクセスできるさまざまなコンピュータ設定を管理できます。

ブート オプションの管理

BIOS Configuration を使用して、コンピュータの電源を入れるか再起動したときに実行されるタスクのさまざまな設定を管理できます。

ブート オプションを管理するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択します。
3. BIOS 管理者パスワード プロンプトで Computer Setup 管理者パスワードを入力し、**[OK]** をクリックします。

注記　BIOS 管理者パスワード プロンプトは、Computer Setup セットアップ パスワードが設定されている場合のみ表示されます。Computer Setup セットアップ パスワードについて詳細しくは、この章の後半の「セットアップ パスワードの設定」を参照してください。

4. 左側のペインで、**[System Configuration]** (システム構成) を選択します。
5. 右側のペインで、F9、F10、F12 の各キー、および **[Express Boot Popup Delay (Sec)]** (Express Boot ポップアップの遅延 (秒)) で使用される遅延時間 (秒単位) を選択します。
6. **[MultiBoot]** (マルチブート) を有効または無効にします。
7. マルチブートを有効にした場合は、一覧からブート デバイスを選択し、上向き矢印または下向き矢印をクリックして順序を調整することにより、ブート順序を選択します。
8. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

システム構成オプションの有効化と無効化

注記　以下の項目の一部は、機種によってはサポートされない場合があります。

デバイスまたはセキュリティ オプションを有効または無効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択します。
3. BIOS 管理者パスワード プロンプトで Computer Setup 管理者パスワードを入力し、**[OK]** をクリックします。
4. 左側のペインで、**[System Configuration]** (システム構成) を選択し、システム構成オプションを有効または無効にするか、右側のペインで以下のシステム構成オプションを設定します。
   - ポート オプション
     - シリアル ポート
     - 赤外線ポート
     - パラレル ポート
     - SD スロット
     - USB ポート
     - 1394 ポート
     - カードバス スロット
     - ExpressCard スロット
   - ブート オプション
     - F9、F10、および F12 の遅延 (秒単位)
     - マルチブート
     - Express Boot ポップアップの遅延 (秒単位)
     - CD-ROM ブート
     - フロッピー ブート
     - 内蔵ネットワーク アダプタ ブート
     - 内蔵ネットワーク アダプタ ブート モード (PXE または RPL)
     - ブート順序
   - デバイス構成
     - ブート時の Num Lock
     - Fn/Ctrl キーの入れ替え
     - 複数のポインティング デバイス

- USB のレガシ サポート
- パラレル ポート モード (標準、双方向、EPP、または ECP)
- データ実行禁止
- SATA ネイティブ モード
- デュアル コア CPU
- Automatic Intel® SpeedStep 機能のサポート
- AC 電源での動作時は常にファンをオンにする
- BIOS DMA データ転送
- Intel または AMD PSAE 実行無効設定

- 内蔵デバイス オプション
    - 内蔵 WLAN デバイスの無線通信
    - 内蔵 WWAN デバイスの無線通信
    - 内蔵 Bluetooth® デバイスの無線通信
    - LAN/WLAN の切り替え
    - 電源オフ状態からの Wake on LAN の実行

5. 変更を保存して終了するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

高度なタスク

ProtectTools の各種設定の管理

ProtectTools セキュリティ マネージャの一部の機能は、BIOS Configuration でも管理できます。

スマート カードまたは Java Card の電源投入時認証サポートの有効化と無効化

このオプションを有効にすると、コンピュータの電源を入れたときに、スマート カードまたは Java Card を使用してユーザー認証を行うことができます。

注記　この電源投入時認証機能を完全に有効にするには、Smart Card Security for ProtectTools または Java Card Security for ProtectTools モジュールを使用してスマート カードを設定する必要があります。

スマート カードの電源投入時認証サポートを有効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択します。
3. BIOS 管理者パスワード プロンプトで Computer Setup 管理者パスワードを入力し、**[OK]** をクリックします。
4. 左側のペインで、**[Security]** (セキュリティ) を選択します。
5. **[Smart Card Security]** の **[Enable]** (有効化) を選択します。

   注記　スマート カードの電源投入時認証を無効にするには、**[Disable]** (無効化) を選択します。

6. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

Embedded Security での電源投入時認証サポートの有効化と無効化

このオプションを有効にすると、コンピュータの電源を入れたときに、TPM 内蔵セキュリティ チップを使用してユーザー認証を行うことができます (使用可能な場合) 。

注記　この電源投入時認証機能を完全に有効にするには、Embedded Security for ProtectTools モジュールを使用して TPM 内蔵セキュリティ チップを設定する必要があります。

Embedded Security での電源投入時認証サポートを有効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択します。
3. BIOS 管理者パスワード プロンプトで Computer Setup 管理者パスワードを入力し、**[OK]** をクリックします。
4. 左側のペインで、**[Security]** (セキュリティ) を選択します。
5. **[Embedded Security]** で、**[Enable Power-on Authentication Support]** (電源投入時認証の有効化) を選択します。

   注記　Embedded Security で電源投入時認証を無効にするには、**[Disable]** (無効化) を選択します。

6. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

自動 DriveLock によるハード ドライブの保護の有効化と無効化

このオプションを有効にすると、DriveLock パスワードが自動的に生成されてドライブに設定され、TPM 内蔵セキュリティ チップによって保護されます。

注記　自動生成されたパスワードがドライブに設定されるのは、コンピュータを再起動し、パスワード プロンプトで正しい TPM 内蔵セキュリティ パスワードを入力した後です。

自動 DriveLock を有効にするオプションを使用するには、以下の条件があります。

- コンピュータに TPM セキュリティ チップが搭載され、初期化されている。TPM セキュリティ チップの有効化と初期化方法については、第 4 章「Embedded Security for ProtectTools」の 内蔵セキュリティ チップの有効化 」と「内蔵セキュリティ チップの初期化」を参照してください。
- 有効になっている DriveLock パスワードがない。

注記　DriveLock パスワードを手動で既に設定している場合は、自動 DriveLock 保護を設定する前に、手動で設定したパスワードを無効にする必要があります。

自動 DriveLock 保護を有効または無効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択します。
3. BIOS 管理者パスワード プロンプトで Computer Setup 管理者パスワードを入力し、**[OK]** をクリックします。
4. 左側のペインで、**[Security]** (セキュリティ) を選択します。
5. **[Embedded Security]** で、**[Automatic DriveLock Support]** (自動 DriveLock) の横の **[Enable]** (有効化) を選択します。

   注記　Embedded Security で自動 DriveLock 保護を無効にするには、**[Disable]** (無効化) を選択します。

6. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

Computer Setup のパスワードの管理

BIOS Configuration を使用して、Computer Setup の電源投入時パスワードとセットアップ パスワードを設定および変更できます。また、さまざまなパスワード設定を管理できます。

注意　BIOS Configuration の [Passwords] (パスワード) ページで設定したパスワードは、ProtectTools ウィンドウで **[Apply]** (適用) または **[OK]** をクリックするとすぐに保存されます。パスワードを取り消すには前のパスワードを指定する必要があるため、設定したパスワードを忘れないようにしてください。

電源投入時パスワードによって、コンピュータの不正使用を防止できます。

注記　電源投入時パスワードを設定すると、[Passwords] (パスワード) ページの [Set] (設定) ボタンは [Change] (変更) ボタンに置き換わります。

Computer Setup のセットアップ パスワードは、Computer Setup の各種設定とシステム識別情報を保護します。このパスワードを設定した後で Computer Setup にアクセスするには、パスワードを入力する必要があります。セットアップ パスワードを設定した場合は、BIOS Configuration for ProtectTools を開くときにパスワードの入力を求められます。

注記 セットアップ パスワードを設定すると、[Passwords] (パスワード) ページの [Set] (設定) ボタンは [Change] (変更) ボタンに置き換わります。

電源投入時パスワードの設定

電源投入時パスワードを設定するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択し、**[Security]** (セキュリティ) を選択します。
3. 右側のペインで、**[Power-On Password]** (電源投入時パスワード) の横の **[Set]** (設定) をクリックします。
4. **[Enter Password]** (パスワードの入力) ボックスと **[Verify Password]** (パスワードの確認) ボックスにパスワードを入力します。
5. [Passwords] (パスワード) ダイアログ ボックスで **[OK]** をクリックします。
6. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

電源投入時パスワードの変更

電源投入時パスワードを変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択し、**[Security]** (セキュリティ) を選択します。
3. 右側のペインで、**[Power-On Password]** (電源投入時パスワード) の横の **[Change]** (変更) をクリックします。
4. **[Old password]** (古いパスワード) ボックスに現在のパスワードを入力します。
5. **[Enter New Password]** (新しいパスワードを入力) ボックスに新しいパスワードを設定して確認します。
6. **[Passwords]** (パスワード) ダイアログ ボックスで **[OK]** をクリックします。
7. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

セットアップ パスワードの設定

Computer Setup のセットアップ パスワードを設定するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択し、**[Security]** (セキュリティ) を選択します。
3. 右側のペインで、**[Setup Password]** (セットアップ パスワード) の横の **[Set]** (設定) をクリックします。

4. **[Enter Password]** (パスワードの入力) ボックスと **[Confirm Password]** (パスワードの確認) ボックスにパスワードを入力します。

5. **[Passwords]** (パスワード) ダイアログ ボックスで **[OK]** をクリックします。

6. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

セットアップ パスワードの変更

Computer Setup のセットアップ パスワードを変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。

2. 左側のペインで、**[BIOS Configuration]** を選択し、**[Security]** (セキュリティ) を選択します。

3. 右側のペインで、**[Setup Password]** (セットアップ パスワード) の横の **[Change]** (変更) をクリックします。

4. **[Old password]** (古いパスワード) ボックスに現在のパスワードを入力します。

5. **[Enter New Password]** (新しいパスワードの入力) ボックスと **[Verify New Password]** (新しいパスワードの確認) ボックスにパスワードを入力します。

6. **[Passwords]** (パスワード) ダイアログ ボックスで **[OK]** をクリックします。

7. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

パスワード オプションの設定

BIOS Configuration for ProtectTools を使用してパスワード オプションを設定すると、システムのセキュリティを強化できます。

厳重セキュリティの有効化または無効化

注意 コンピュータが永久に使用不能になる事態を回避するために、設定したセットアップ パスワード、電源投入時パスワード、またはスマート カード PIN をコンピュータとは別の安全な場所に記録しておいてください。これらのパスワードまたは PIN を使用しないと、コンピュータのロックを解除することはできません。

厳重セキュリティを有効にすると、電源投入時パスワードや管理者パスワードおよびその他の形式の電源投入時認証に対する保護が強化されます。

厳重セキュリティを有効または無効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。

2. 左側のペインで、**[BIOS Configuration]** を選択し、**[Security]** (セキュリティ) を選択します。

3. 右側のペインで、**[Password Options]** (パスワード オプション) の **[Stringent Security]** (厳重セキュリティ) を有効または無効にします。

注記　厳重セキュリティを無効にする場合は、**[Enable Stringent Security]** (厳重セキュリティの有効化) チェック ボックスをオフにします。

4. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

Windows 再起動時の電源投入時認証の有効化と無効化

このオプションを使用すると、Windows の再起動時に、電源投入時、TPM、またはスマート カード パスワードを入力するようにユーザーに要求することによって、セキュリティを強化できます。

Windows 再起動時の電源投入時認証を有効または無効にするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[BIOS Configuration]** を選択し、**[Security]** (セキュリティ) を選択します。
3. 右側のペインで、**[Password Options]** (パスワード オプション) の **[Require password on restart]** (再起動時にパスワードが必要) を有効または無効にします。
4. 変更を保存するには、ProtectTools ウィンドウで **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

6 Credential Manager for ProtectTools

Credential Manager for ProtectTools には、コンピュータに対する不正アクセスを防止する以下のセキュリティ機能があります。

- Microsoft Windows にログインするときにパスワードの代わりにスマート カードやバイオメトリック リーダーなどを使用してログインする機能。詳しくは、この章の後半の「資格情報の登録」を参照してください。
- Web サイト、アプリケーション、および保護されたネットワーク リソースのための資格情報を自動的に記憶するシングル サインオン機能。
- スマート カードやバイオメトリック リーダーなどの別売のセキュリティ デバイスのサポート。
- コンピュータのロック解除に別売のセキュリティ デバイスを使用した認証を要求するなど、追加のセキュリティ設定のサポート。

セットアップ手順

Credential Manager へのログオン

設定に応じて、以下のいずれかの方法で Credential Manager にログオンできます。

- Credential Manager ログオン ウィザード (推奨)
- 通知領域にある Credential Manager アイコン
- ProtectTools セキュリティ マネージャ

注記 Windows ログオン画面で Credential Manager ログオン プロンプトを使用して Credential Manager にログオンすると、Windows にも同時にログオンできます。

初めてのログオン

Credential Manager を初めて開くときは、通常の Windows ログオン パスワードを使用してログオンします。Credential Manager アカウントは、Windows ログオン資格情報を使用して自動的に作成されます。

Credential Manager にログオンした後、指紋やスマート カードなどの追加の資格情報を登録できます。詳しくは、この章の後半の「資格情報の登録」を参照してください。

次回のログオン時にログオン ポリシーを選択し、登録した資格情報を任意に組み合わせて使用できます。

Credential Manager ログオン ウィザードの使用

Credential Manager ログオン ウィザードを使用して Credential Manger にログオンするには、次の手順を行います。

1. 以下のいずれかの方法で、Credential Manager ログオン ウィザードを開きます。
   - Windows ログオン画面からログオン。
   - 通知領域にある ProtectTools アイコンをダブルクリックする。
   - ProtectTools セキュリティ マネージャの [Credential Manager] ページで、ウィンドウの右上にある **[Log On]** (ログオン) のリンクをクリックする。
2. **[Next]** (次へ) をクリックします。
3. **[User name]** (ユーザー名) ボックスにユーザー名を入力し、**[Next]** (次へ) をクリックします。
4. **[Password]** (パスワード) ボックスにパスワードを入力し、**[Next]** (次へ) をクリックします。
5. 画面に表示される手順に従って、選択した認証方法を使用してログオンします。
6. **[Finish]** (終了) をクリックします。

アカウントの新規作成

Credential Manager ログオン ウィザードを使用して、新しいユーザー アカウントを作成できます。操作を開始するには、管理者アカウントで Windows にログオンしている必要があります (ただし、Credential Manager にはログオンしていない状態)。

アカウントを新規作成するには、次の手順を行います。

1. 通知領域のアイコンをダブルクリックして、Credential Manager を開きます。Credential Manager ログオン ウィザードが開きます。
2. [Introduce Yourself] (自己紹介) ページで **[More]** (その他) をクリックし、**[Sign Up for a New Account]** (新規アカウントのサインアップ) をクリックします。
3. **[Next]** (次へ) をクリックします。
4. [Registration] (登録) ページで、ユーザー名とアカウントの説明を入力します。
5. **[Next]** (次へ) をクリックします。
6. [Authentication Methods] (認証方法) ページで、登録する認証方法を選択し、登録しない認証方法のチェック ボックスをオフにして、**[Next]** (次へ) をクリックします。
7. 画面に表示される手順に従って、選択した資格情報を登録します。
8. **[Finish]** (終了) をクリックします。

資格情報の登録

[My Identity] (自分の ID) ページを使用して、さまざまな認証方法 (資格情報) を登録できます。認証方法を登録した後、登録した方法を使用して Credential Manager にログオンできます。

指紋の登録

指紋リーダーを使用すると、Windows パスワードの代わりに ProtectTools セキュリティ マネージャに登録した指紋を使用して Microsoft Windows にログオンできます。

指紋リーダーを内蔵した HP コンピュータを使用している場合でも、別売の指紋リーダーを使用している場合でも、指紋リーダーを使用して Windows にログインするには、以下の 2 つの手順を実行する必要があります。

- 指紋リーダーを設定します。
- 登録した指紋を使用して Windows にログオンします。

指紋リーダーのセットアップ

注記　別売の指紋リーダーを使用する場合は、以下の手順を実行する前に、コンピュータにリーダーを接続してください。

指紋リーダーをセットアップするには、次の手順を行います。

1. Windows で、タスクバーの通知領域にある **[Credential Manager]** アイコンをダブルクリックします。

   - または -

   [スタート > すべてのプログラム > ProtectTools Security Manager] の順に選択し、左側のペインの **[Credential Manager]** をクリックします。

2. [My Identity] (自分の ID) ページで、ページの右上隅にある **[Log On]** (ログオン) をクリックします。

   Credential Manager ログオン ウィザードが開きます。

3. [Introduce Yourself] (自己紹介) ページで、**[Next]** (次へ) をクリックしてデフォルトのユーザー名をそのまま使用します。

   注記　このコンピュータに他のユーザーが登録されている場合は、Windows ユーザー名を入力することによって、指紋を登録する必要があるユーザーを選択できます。

4. [Enter Password] (パスワードの入力) ページで、ユーザーの Windows パスワードが設定されている場合は、パスワードを入力します。それ以外の場合は、**[Finish]** (終了) をクリックします。

5. [My Services and Applications] (サービスとアプリケーション) ページで、**[Register Fingerprints]** (指紋の登録) をクリックします。

   注記　デフォルトでは、*少なくとも*異なる 2 本の指の指紋を登録する必要があります。

6. Credential Manager 登録ウィザードが開いているときに、指紋センサーに指をゆっくりと押し付けます。

   注記　デフォルトでは、右手の人差し指を 1 つ目の指紋として登録します。左手または右手の最初に登録する指をクリックすると、このデフォルトを変更できます。いずれかの指をクリックすると、その指の輪郭が強調表示されて、選択されたことが示されます。

7. 画面上の指が緑色に変わるまで、同じ指を指紋センサーに押し付けたままにします。

   注記　1 回の読み取りが終わるたびに進捗インジケータが先に進みます。1 本の指の指紋を登録するために複数回の読み取りが必要です。

   注記　指紋登録処理中に始めからやり直す必要がある場合は、画面上の強調表示されている指を右クリックし、**[Start Over]** (やり直し) をクリックします。

8. 次に登録する別の指を画面上でクリックし、手順 6 と 7 を繰り返します。

   注記　少なくとも 2 本の指を登録する前に **[Finish]** (終了) をクリックすると、エラー メッセージが表示されます。続行するには、**[OK]** をクリックします。

9. 少なくとも 2 本の指を登録した後、**[Finish]** (終了) をクリックし、**[OK]** をクリックします。

10. 別の Windows ユーザーのために指紋リーダーを設定するには、そのユーザーとして Windows にログオンし、手順 1 ～ 9 を繰り返します。

登録した指紋を使用しての Windows へのログオン

登録した指紋を使用して Windows にログオンするには、次の手順を行います。

1. 指紋登録の直後に、Windows を再起動します。

2. 画面の左上にある **[Log on to Credential Manager]** (Credential Manager へのログオン) をクリックします。

3. [Credential Manager Logon Wizard] ダイアログ ボックスで、ユーザー名をクリックする代わりに、登録済みのいずれかの指を使用して Windows にログオンします。

4. Windows パスワードを入力して、指紋とパスワードを関連付けます。

注記　指紋を使用して初めて Windows にログオンしたとき、Windows パスワードが設定されている場合は、Windows パスワードと指紋を関連付けるためにパスワードを入力する必要があります。パスワードと指紋を関連付けた後は、指紋リーダーを使用するときに再度パスワードを入力する必要はありません。

スマート カードまたはトークンの登録

スマート カードまたはトークンを登録するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。

2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。

3. 右側のペインで、**[I Want To]** (実行する操作) の **[Register Smart Card or Token]** (スマート カードまたはトークンの登録) をクリックします。

4. **[Next]** (次へ) をクリックします。

5. 登録する認証方法をクリックし、**[Next]** (次へ) をクリックします。

6. 画面に表示される手順に従って、登録を完了します。

他の資格情報の登録

他の資格情報を登録するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。

2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。

3. 右側のペインで、**[I Want To]** (実行する操作) の **[More]** (その他) をクリックし、**[Register Credentials]** (資格情報の登録) をクリックします。

4. 登録する認証方法をクリックし、**[Next]** (次へ) をクリックします。

5. 画面に表示される手順に従って、登録を完了します。

全般的なタスク

Credential Manager の [My Identity] (自分の ID) ページは、すべてのユーザーがアクセスできます。[My Identity] (自分の ID) ページから、以下の操作を実行できます。

- 認証資格情報の作成と登録
- パスワードの管理
- Microsoft ネットワーク アカウントの管理
- シングル サインオン資格情報の管理

仮想トークンの作成

仮想トークンは、スマート カードや USB トークンと同様の機能を果たします。トークンはコンピューターのハード ドライブまたは Windows レジストリに保存されます。仮想トークンを使用してログオンすると、認証を完了するためにユーザー PIN の入力が要求されます。

仮想トークンを新規作成するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[I Want To]** (実行する操作) の **[More]** (その他) をクリックし、**[Register Credentials]** (資格情報の登録) をクリックします。
4. **[Next]** (次へ) をクリックします。
5. **[Virtual Token]** (仮想トークン) をクリックし、**[Next]** (次へ) をクリックします。
6. **[Create New]** (新規作成) をクリックし、**[Next]** (次へ) をクリックします。
7. 仮想トークン ファイルの名前と場所を入力 (または **[Browse]** (参照) をクリックしてファイルの場所を検索) し、**[Next]** (次へ) をクリックします。
8. マスタ PIN とユーザー PIN を設定して確認します。
9. **[Finish]** (終了) をクリックします。

Windows ログオン パスワードの変更

Credential Manager の [My Identity] (自分の ID) ページから Windows ログオン パスワードを変更できます。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[I Want To]** (実行する操作) の **[Change Windows Logon Password]** (Windows ログオン パスワードの変更) をクリックします。
4. **[Old password]** (古いパスワード) ボックスに現在のパスワードを入力します。
5. **[New Password]** (新しいパスワード) ボックスと **[Confirm password]** (パスワードの確認) ボックスでパスワードを設定して確認します。
6. **[Finish]** (終了) をクリックします。

トークン PIN の変更

Credential Manager の [My Identity] (自分の ID) ページからスマート カードまたは仮想トークンの PIN を変更できます。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[I Want To]** (実行する操作) の **[More]** (その他) をクリックし、**[Change Token PIN]** (トークン PIN の変更) をクリックします。
4. **[Next]** (次へ) をクリックします。
5. PIN を変更するトークンを選択し、**[Next]** (次へ) をクリックします。
6. 画面に表示される手順に従って、PIN の変更を完了します。

ID の管理

ID のバックアップ

データの消失や間違って削除した場合に備えて、Credential Manager で ID をバックアップしておくことをお勧めします。

ID をバックアップするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[I Want To]** (実行する操作) の **[More]** (その他) をクリックし、**[Backup Identity]** (ID のバックアップ) をクリックします。
4. **[Next]** (次へ) をクリックします。
5. バックアップする要素を選択し、**[Next]** (次へ) をクリックします。
6. [Device Type] (デバイス タイプ) ページで、バックアップを復元するために使用するデバイスの種類を選択し、**[Next]** (次へ) をクリックします。

   注記　バックアップ ファイル用に選択したデバイスのパスワードまたは PIN コードを知っている必要があります。

7. 選択したデバイスに関する画面の説明に沿って操作し、**[Finish]** (終了) をクリックします。

ID の復元

ID を復元するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[I Want To]** (実行する操作) の **[More]** (その他) をクリックし、**[Restore Identity]** (ID の復元) をクリックします。
4. **[Next]** (次へ) をクリックします。
5. [Device Type] (デバイス タイプ) ページで、バックアップが保存されているデバイスの種類を選択し、**[Next]** (次へ) をクリックします。
6. 選択したデバイスに関する画面の説明に沿って操作し、**[Finish]** (終了) をクリックします。
7. 確認ダイアログ ボックスで **[Yes]** (はい) をクリックします。

システムからの ID の削除

Credential Manager から ID を完全に削除できます。

注記 この操作は、Windows ユーザー アカウントには影響しません。

システムから ID を削除するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[I Want To]** (実行する操作) の **[More]** (その他) をクリックし、**[Remove My Identity from the System]** (システムから ID を削除する) をクリックします。
4. 確認ダイアログ ボックスで **[Yes]** (はい) をクリックします。ID がログオフされ、システムから削除されます。

コンピュータのロック

ワークステーション ロック機能を使用すると、離席中にコンピュータを保護することができます。ワークステーション ロック機能によって、権限のないユーザーがコンピュータにアクセスできないようにすることができます。コンピュータのロック解除は、そのコンピュータのユーザー自身と管理者グループだけが実行できます。

注記　セキュリティを強化するために、ワークステーション ロック機能を使用して、スマートカード、バイオメトリック リーダー、またはトークンがないとコンピュータのロックを解除できないように設定できます。詳しくは、この章の後半の「Credential Manager プログラムの設定の指定」を参照してください。

コンピュータをロックするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[I Want To]** (実行する操作) の **[More]** (その他) をクリックし、**[Lock Workstation]** (ワークステーションのロック) をクリックします。Windows ログオン画面が表示されます。コンピュータのロックを解除するには、Windows パスワードまたは Credential Manager ログオン ウィザードを使用する必要があります。

注記　コンピュータのロックを解除するには、Windows パスワードまたは Credential Manager ログオン ウィザードを使用する必要があります。

Microsoft ネットワーク ログオンの使用

Credential Manager を使用して、ローカル コンピュータまたはネットワーク ドメインで Windows にログオンできます。Credential Manager に初めてログオンしたときに、ローカルの Windows ユーザー アカウントがネットワーク ログオン サービスのネットワーク アカウントとして自動的に追加されます。詳しくは、この章の前半の「初めてのログオン」を参照してください。

Credential Manager を使用した Windows へのログオン

Credential Manager を使用して、Windows のネットワークまたはローカル アカウントにログオンできます。

1. Windows ログオン画面で、**[Log on to Credential Manager]** (Credential Manager へのログオン) をクリックします。
2. [Welcome] (ようこそ) ページが表示された場合は、**[Next]** (次へ) をクリックします。
3. **[User name]** (ユーザー名) ボックスにユーザー名を入力します。

   注記　このユーザー名をデフォルトのユーザー名にする場合は、**[Use this name next time you log on]** (次回ログオン時にこの名前を使用する) チェック ボックスをオンにします。

4. **[Log on to]** (ログオン先) の一覧から **[Credential Manager]** を選択します。
5. **[Next]** (次へ) をクリックします。[Logon Policy] (ログオン ポリシー) ページで、使用する認証方法を選択します。

注記 この方法をデフォルトの方法にする場合は、**[Use this policy next time you log on]** (次回ログオン時にこのポリシーを使用する) チェック ボックスをオンにします。

6. 選択した認証方法に関する画面の説明に沿って操作します。認証情報が正しい場合は、Windows アカウントと Credential Manager にログオンできます。

アカウントの追加

Credential Manager にログオンした後、ローカルまたはドメイン アカウントを追加できます。

アカウントを追加するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[Microsoft Network Logon]** (Microsoft ネットワーク ログオン) の **[Add a Network Account]** (ネットワーク アカウントの追加) をクリックします。
4. **[User name]** (ユーザー名) ボックスに新しいアカウントのユーザー名を入力します。
5. 使用できるドメインの一覧からドメインを選択します。
6. パスワードを入力して確認します。

注記 このアカウントをデフォルトのユーザー アカウントにする場合は、**[Use these credentials by default]** (デフォルトでこれらの資格情報を使用する) チェック ボックスをオンにします。

7. **[Finish]** (終了) をクリックします。

アカウントの削除

Credential Manager にログオンした後、ローカルまたはドメイン アカウントを削除できます。

アカウントを削除するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[Microsoft Network Logon]** (Microsoft ネットワーク ログオン) の **[Manage Network Account]** (ネットワーク アカウントの管理) をクリックします。
4. 削除するアカウントをクリックし、**[Remove]** (削除) をクリックします。
5. 確認ダイアログ ボックスで **[Yes]** (はい) をクリックします。

デフォルト ユーザーの設定

Credential Manager にログオンした後、デフォルト ユーザーを設定または変更できます。

デフォルト ユーザーを設定するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。

3. 右側のペインで、**[Microsoft Network Logon]** (Microsoft ネットワーク ログオン) の **[Manage Network Account]** (ネットワーク アカウントの管理) をクリックします。

4. デフォルトにするアカウントをクリックし、**[Properties]** (プロパティ) をクリックします。

5. **[Account Properties]** (アカウントのプロパティ) ダイアログ ボックスの **[Set Up Account]** (アカウントの設定) タブで、**[Use these credentials by default]** (デフォルトでこれらの資格情報を使用する) チェック ボックスをオンにします。

6. **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

シングル サインオンの使用

Credential Manager には、複数のインターネット アプリケーションおよび Windows アプリケーションのユーザー名とパスワードを保存しておき、登録したアプリケーションへのアクセス時にログオン資格情報を自動的に入力するシングル サインオン機能があります。

注記 セキュリティとプライバシーの保護はシングル サインオンの重要な特性です。すべての資格情報は暗号化され、Credential Manager へのログオンが成功した後でのみ使用可能になります。

注記 セキュリティで保護されたサイトやアプリケーションにログオンする前にスマート カード、バイオメトリック リーダー、またはトークンを使用して認証資格情報を検証するようにシングル サインオンを設定することもできます。これは、銀行の口座番号などの個人情報を含むアプリケーションや Web サイトにログオンするときに、特に役に立ちます。詳しくは、この章の後半の「Credential Manager プログラムの設定の指定」を参照してください。

新しいアプリケーションの登録

Credential Manager にログオンした状態で起動するすべてのアプリケーションに対して、登録を求めるメッセージが表示されます。手動でアプリケーションを登録することもできます。

自動登録機能の使用

自動登録機能を使用してアプリケーションを登録するには、次の手順を行います。

1. ログオンする必要があるアプリケーションを開きます。

2. **[Credential Manager Single Sign On]** (Credential Manager シングル サインオン) ダイアログ ボックスで、**[Options]** (オプション) をクリックして、次の登録設定を指定します。

   - このサイトまたはアプリケーションでは SSO を使用するように指示しない。
   - 資格情報だけを入力する。送信しない。
   - 資格情報を送信する前に確認する。

3. **[Yes]** (はい) をクリックして登録を完了します。

手動 (ドラッグ アンド ドロップ) での登録

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。

2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。

3. 右側のペインで、**[Single Sign On]** (シングル サインオン) の **[Register New Application]** (新しいアプリケーションの登録) をクリックします。

4. パスワード ダイアログ ボックスがあるページが表示されるまで、登録するアプリケーションを実行します。
5. SSO 登録ウィザードの [Drag and Drop Registration] (ドラッグ アンド ドロップでの登録) ページで、自動化するアクティビティのタイプを選択します。

   注記　ほとんどの場合、自動化するアクティビティは **[Logon dialog]** (ログオン ダイアログ) になります。

6. ウィザードのページでアイコンをクリックし、パスワード ボックスがあるアプリケーションの領域にドラッグします。領域が強調表示されたら、マウスのボタンを離します。

   注記　ページ上を移動する間は指のアイコンは表示されませんが、アプリケーションのログオン ボックス上にポインタをドラッグすると、長方形のアイコンが表示されます。

7. SSO 登録ウィザードの [Application Information] (アプリケーション情報) ページで、アプリケーションの名前と説明を入力します。
8. **[Finish]** (終了) をクリックします。
9. アプリケーション ボックスにログオン資格情報 (ユーザー名やパスワードなど) を入力します。
10. 確認ダイアログ ボックスで、資格情報の名前を確認または修正し、**[Yes]** (はい) をクリックします。

アプリケーションと資格情報の管理

アプリケーションのプロパティの変更

アプリケーションのプロパティを変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[Single Sign On]** (シングル サインオン) の **[Manage Applications and Credentials]** (アプリケーションと資格情報の管理) をクリックします。
4. 変更するアプリケーションのエントリをクリックし、**[プロパティ]** をクリックします。
5. アプリケーションの名前と説明を変更するには、**[General]** (全般) タブをクリックします。該当する設定の横にあるチェック ボックスをオンまたはオフにすることによって、設定を変更します。
6. SSO アプリケーション スクリプトを表示および編集するには、**[Script]** (スクリプト) タブをクリックします。
7. 変更を保存するには、**[OK]** をクリックします。

シングル サインオンからのアプリケーションの削除

シングル サインオンからアプリケーションを削除するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。

3. 右側のペインで、**[Single Sign On]** (シングル サインオン) の **[Manage Applications and Credentials]** (アプリケーションと資格情報の管理) をクリックします。
4. 削除するアプリケーションをクリックし、**[Remove]** (削除) をクリックします。
5. 確認ダイアログ ボックスで **[Yes]** (はい) をクリックします。
6. **[OK]** をクリックします。

アプリケーションのエクスポート

アプリケーションをエクスポートして、シングル サインオン アプリケーション スクリプトのバックアップ コピーを作成できます。このファイルは、シングル サインオン データの回復に使用できます。このファイルは、資格情報だけを保存した ID バックアップ ファイルを補足する働きをします。

アプリケーションをエクスポートするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[Single Sign On]** (シングル サインオン) の **[Manage Applications and Credentials]** (アプリケーションと資格情報の管理) をクリックします。
4. エクスポートするアプリケーションのエントリをクリックします。**[More]** (その他) をクリックし、**[Export Application]** (アプリケーションのエクスポート) をクリックします。
5. 画面に表示される手順に従って、エクスポートを完了します。
6. **[OK]** をクリックします。

アプリケーションのインポート

アプリケーションをインポートするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[Single Sign On]** (シングル サインオン) の **[Manage Applications and Credentials]** (アプリケーションと資格情報の管理) をクリックします。
4. インポートするアプリケーション エントリをクリックします。**[More]** (その他) をクリックし、**[Import Application]** (アプリケーションのインポート) をクリックします。
5. 画面に表示される手順に従って、インポートを完了します。
6. **[OK]** をクリックします。

資格情報の変更

資格情報を変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[My Identity]** (自分の ID) を選択します。
3. 右側のペインで、**[Single Sign On]** (シングル サインオン) の **[Manage Applications and Credentials]** (アプリケーションと資格情報の管理) をクリックします。

4. 変更するアプリケーションのエントリをクリックし、**[More]** (その他) をクリックします。
5. 以下のオプションのいずれかを選択します。
   - **[Add New Credentials]** (新しい資格情報を追加する)
   - **[Delete Credentials]** (資格情報を削除する)
   - **[Delete Unused Credentials]** (使用されていない資格情報を削除する)
   - **[Edit Credentials]** (資格情報を編集する)
6. 画面に表示される手順に従います。
7. 変更を保存するには、**[OK]** をクリックします。

高度なタスク (管理者専用)

Credential Manager の [Authentication and Credentials] (認証と資格情報) ページと [Advanced Settings] (詳細設定) ページは、管理者権限があるユーザーだけが使用できます。これらのページから、以下の操作を実行できます。

- ユーザーと管理者のログオン方法の指定
- 資格情報のプロパティの設定
- Credential Manager プログラムの設定値の指定

ユーザーと管理者のログオン方法の指定

[Authentication and Credentials] (認証と資格情報) ページから、ユーザーと管理者のそれぞれに必要な資格情報の種類や組み合わせを指定できます。

ユーザーまたは管理者のログオン方法を指定するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[Authentication and Credentials]** (認証と資格情報) を選択します。
3. 右側のペインで、**[Authentication]** (認証) タブをクリックします。
4. カテゴリの一覧からカテゴリ (**[Users]** (ユーザー) または **[Administrators]** (管理者)) を選択します。
5. 認証方法の一覧から、認証の種類または組み合わせを選択します。
6. **[OK]** をクリックします。
7. 変更を保存するには、**[Apply]** (適用) をクリックし、**[OK]** をクリックします。

カスタム認証要件の設定

[Authentication and Credentials] (認証と資格情報) ページに目的の認証資格情報セットが含まれていない場合は、カスタム要件を作成できます。

カスタム要件を設定するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[Authentication and Credentials]** (認証と資格情報) を選択します。
3. 右側のペインで、**[Authentication]** (認証) タブをクリックします。
4. カテゴリの一覧からカテゴリ (**[Users]** (ユーザー) または **[Administrators]** (管理者)) を選択します。
5. 認証方法の一覧の **[Custom]** (カスタム) をクリックします。
6. **[設定]** をクリックします。
7. 使用する認証方法を選択します。
8. 以下のいずれかをクリックして組み合わせ方法を選択します。
   - 認証方法を AND で組み合わせる

     (ユーザーがログインするたびに、指定したすべての方法でユーザーを認証する必要があります。)
   - 認証方法を OR で組み合わせる

     (ユーザーがログオンするたびに、指定した方法のいずれかを認証方法としてユーザーが選択できます。)
9. **[OK]** をクリックします。
10. 変更を保存するには、**[Apply]** (適用) をクリックし、**[OK]** をクリックします。

資格情報のプロパティの設定

[Authentication and Credentials] (認証と資格情報) ページの [Credentials] (資格情報) タブから、認証方法の一覧を表示し、設定を変更できます。

資格情報を設定するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[Authentication and Credentials]** (認証と資格情報) を選択します。
3. 右側のペインで、**[Credentials]** (資格情報) タブをクリックします。

4. 変更する資格情報の種類をクリックします。
   - 資格情報を登録するには、**[Register]** (登録) をクリックし、画面に表示される手順に従います。
   - 資格情報を削除するには **[Clear]** (消去) をクリックし、確認ダイアログ ボックスで **[Yes]** (はい) をクリックします。
   - 資格情報のプロパティを変更するには、**[Properties]** (プロパティ) をクリックし、画面に表示される手順に従います。
5. **[Apply]** (適用) をクリックし、**[OK]** をクリックします。

Credential Manager プログラムの設定の指定

[Advanced Settings] (詳細設定) ページから、以下のタブを使用してさまざまな設定を変更できます。

- [General] (全般) - 基本的な設定を変更できます。
- [Single Sign On] (シングル サインオン) - 現在のユーザーに対して適用されるシングル サインオンの設定を変更できます。ログオン画面の検出方法、登録済みのダイアログへの自動ログオン、パスワードの表示などの設定があります。
- [Services and Applications] (サービスとアプリケーション) - 使用可能なサービスを表示し、それらのサービスの設定を変更できます。
- [Biometric Settings] (バイオメトリック設定) - 指紋リーダー ソフトウェアを選択し、指紋リーダーのセキュリティ レベルを調整できます。
- [Smart Cards and Tokens] (スマート カードとトークン) - 使用可能なすべてのスマート カードとトークンを表示し、プロパティを変更できます。

Credential Manager の設定を変更するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[Advanced Settings]** (詳細設定) を選択します。
3. 右側のペインで、変更する設定が含まれる適切なタブをクリックします。
4. 画面に表示される手順に従って、設定を変更します。
5. 変更を保存するには、**[Apply]** (適用) をクリックし、**[OK]** をクリックします。

例 1 - [Advanced Settings] (詳細設定) ページを使用して Credential Manager から Windows にログオンできるようにする

Credential Manager から Windows にログオンできるようにするには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[Advanced Settings]** (詳細設定) を選択します。
3. 右側のペインで、**[General]** (全般) タブをクリックします。
4. **[Use Credential Manager to log on to Windows]** (Credential Manager を使用して Windows にログオンする) チェック ボックスをオンにします。

5. 変更を保存するには、**[Apply]** (適用) をクリックし、**[OK]** をクリックします。
6. コンピュータを再起動します。

例 2 - [Advanced Settings] (詳細設定) ページを使用してシングル サインオンの前にユーザーの検証を要求する

登録済みのダイアログ ボックスまたは Web ページにログオンする前に、シングル サインオンで資格情報の検証を要求するには、次の手順を行います。

1. **[スタート > すべてのプログラム > HP ProtectTools Security Manager]** の順に選択します。
2. 左側のペインで、**[Credential Manager]** を選択し、**[Advanced Settings]** (詳細設定) を選択します。
3. 右側のペインで、**[Single Sign On]** (シングル サインオン) タブをクリックします。
4. **[When registered logon dialog or Web page is visited]** (登録済みのログオン ダイアログまたは Web ページが表示された場合) の **[Validate user before submitting credentials]** (資格情報を送信する前にユーザーを検証する) チェック ボックスをオンにします。
5. 変更を保存するには、**[Apply]** (適用) をクリックし、**[OK]** をクリックします。
6. コンピュータを再起動します。

用語集

BIOS セキュリティ モード (BIOS security mode)　Smart Card Security で行う設定であり、有効にした場合、ユーザー認証にスマート カードの使用と有効な PIN が必要になります。

BIOS プロファイル (BIOS profile)　保存して他のアカウントに適用できる BIOS 構成設定値のグループ。

DriveLock　ハード ドライブをユーザーに関連付け、コンピュータの起動時に正しい DriveLock パスワードの入力をユーザーに要求するセキュリティ機能。

ID (Identity)　ProtectTools Credential Manager において、アカウントやプロファイルのように特定のユーザーについてまとめられた資格情報と設定値のグループ。

Java Card　クレジット カードに似た形と大きさのハードウェアで、所有者に関する識別情報を格納する。コンピュータに対して所有者を認証するために使用される。

USB トークン (USB token)　ユーザーに関する識別情報を格納するセキュリティ デバイス。スマート カードやバイオメトリック リーダーのように、所有者をコンピュータに対して認証するために使用される。

Windows ユーザー アカウント (Windows user account)　ネットワークまたは個々のコンピュータにログオンする権限がある個人のプロファイル。

シングル サインオン (Single Sign On)　認証情報を保存し、パスワード認証が必要なインターネットおよび Windows アプリケーションに Credential Manager を使用してアクセスできるようにする機能。

スマート カード (Smart card)　クレジット カードに似たサイズと形をした小さいハードウェアで、所有者に関する識別情報を格納する。コンピュータに対して所有者を認証するために使用される。

スマート カード ユーザー パスワード (Smart card user password)　Computer Setup でユーザーのスマート カードをコンピュータに関連付け、起動時または再起動時の確認に使用されるパスワード。このパスワードは管理者が手動で設定することも、ランダムに生成することもできる。

スマート カード管理者パスワード (Smart card administrator password)　Computer Setup で管理者のスマート カードをコンピュータに関連付け、起動時または再起動時の確認に使用されるパスワード。このパスワードは管理者が手動で設定することも、ランダムに生成することもできる。

デジタル署名 (Digital signature)　ファイルと共に送信されて、資料の送信元を確認し、署名後のファイルに変更が加えられていないことを確認するデータ。

デジタル証明書 (Digital certificate)　デジタル証明書の所有者の ID と、デジタル情報に署名するために使用される一対の電子キーを結び付けることによって、個人または企業の身元を確認する電子的な資格情報。

ドメイン (Domain)　ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピュータのグループ。ドメインは一意の名前を持ち、各ドメインに共通の規則と手順がある。

トラステッド プラットフォーム モジュール (TPM) 内蔵セキュリティ チップ (Trusted Platform Module (TPM) embedded security chip) (一部のモデルのみ)　悪意のある攻撃者から機密性の高いユーザー情報を保護する内

蔵セキュリティ チップ。ある特定のプラットフォームにおける信頼性の基盤である。TPM は、トラステッド コンピューティング グループ (TCG) の仕様を満たす暗号アルゴリズムと動作を実現する。

ネットワーク アカウント (Network account)　ローカル コンピュータ、ワークグループ、またはドメイン上の Windows ユーザー アカウントまたは管理者アカウント。

パーソナル セキュア ドライブ (Personal secure drive) (PSD)　機密情報のための保護された記憶域を提供する。

バイオメトリック (Biometric)　指紋などの物理的な特徴を利用してユーザーを識別する認証資格情報のカテゴリ。

パブリック キー インフラストラクチャ (Public Key Infrastructure) (PKI)　証明書および暗号キーの作成、使用、管理のためのインタフェースを定義した規格。

リブート (Reboot)　コンピュータを再起動する処理。

暗号サービス プロバイダ (Cryptographic service provider) (CSP)　特定の暗号機能を実行するために、正しく定義されたインタフェースで使用できる暗号アルゴリズムの供給元またはライブラリ。

暗号化 (Encryption)　暗号技術において、権限のない受信者にデータが読まれないように、平文を暗号文に変換するために採用されるアルゴリズムの使用などの手順。多くの種類のデータ暗号化が存在し、それらはネットワーク セキュリティの基礎になっている。一般的な暗号化の種類として、データ暗号化規格とパブリック キー暗号化がある。

暗号化ファイル システム (Encryption File System) (EFS)　選択したフォルダ内のすべてのファイルとサブフォルダを暗号化するシステム。

暗号化解除 (Decryption)　暗号技術において、暗号化されたデータを平文に変換するために使用される手順。

暗号技術 (Cryptography)　特定の個人だけが解読できるようにデータを暗号化および暗号化解除する技術。

移行 (Migration)　キーと証明書の管理、復元、および転送を可能にするタスク。

仮想トークン (Virtual token)　スマート カードおよびスマート カード リーダーとよく似た働きをするセキュリティ機能。トークンはコンピュータのハード ドライブまたは Windows レジストリに保存される。仮想トークンを使用してログオンすると、認証を完了するためにユーザー PIN の入力が要求される。

緊急リカバリ アーカイブ (Emergency recovery archive)　1 つのプラットフォーム所有者キーから別のプラットフォーム所有者キーへの基本ユーザー キーの再暗号化を可能にする保護された記憶域。

厳重セキュリティ (Stringent security)　電源投入時パスワードや管理者パスワードおよびその他の形式の電源投入時認証に対して強化された保護を提供する BIOS Configuration のセキュリティ機能。

資格情報 (Credentials)　認証処理において、特定のタスクに対して必要な資格をユーザーが証明する方法。

自動 DriveLock (Automatic DriveLock)　TPM Embedded Security (内蔵セキュリティ) チップによる DriveLock パスワードの生成と保護を実現するセキュリティ機能。ユーザーが起動時に正しい TPM 基本ユーザー キー パスワードを入力し、TPM 内蔵セキュリティ チップによって認証された場合、BIOS はユーザーに対してハードドライブのロックを解除します。

証明機関 (Certification authority)　パブリック キー インフラストラクチャの運用に必要な証明書を発行するサービス。

電源投入時認証 (Power-on authentication)　コンピュータの電源投入時にスマート カード、セキュリティ チップ、パスワードなどのなんらかの形の認証を要求するセキュリティ機能。

認証 (Authentication)　コンピュータへのアクセス、特定のプログラムの設定の変更、セキュリティで保護されたデータの表示などのタスクを実行する権限がユーザーにあるかどうかを確認する処理。

索引